

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

12/06/2016

SUBJECT:

Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in the Google Android operating system (OS), the most severe of which could allow for remote code execution. Android is an operating system developed by Google for mobile devices including, but not limited to smartphones, tablets, and watches. These vulnerabilities could be exploited through multiple methods such as email, web browsing, and MMS when processing media files. Successful exploitation of these vulnerabilities could result in remote code execution in the context of the application, an attacker gaining elevated privileges, information disclosure, or bypassing security restrictions.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Android OS builds utilizing Security Patch Levels prior to the Security Patch Level published on December 1, 2016.

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: **High**

TECHNICAL SUMMARY:

Google's Android OS is prone to multiple vulnerabilities, the most severe of which could allow for remote code execution. The vulnerabilities are as follows:

- Remote code execution vulnerability in CURL/LIBCURL (CVE-2016-5419, CVE-2016-5420, CVE-2016-5421).

- Elevation of privilege vulnerability in libziparchive (CVE-2016-6762).
- Denial of service vulnerability in Telephony (CVE-2016-6763).
- Denial of service vulnerability in Mediaserver (CVE-2016-6766, CVE-2016-6765, CVE-2016-6764, CVE-2016-6767).
- Remote Code Execution vulnerability in Framesequence library (CVE-2016-6768).
- Elevation of privilege vulnerability in Smart Lock (CVE-2016-6769).
- Elevation of privilege vulnerability in Framework APIs (CVE-2016-6770).
- Elevation of privilege vulnerability in Telephony (CVE-2016-6771).
- Elevation of privilege vulnerability in Wi-Fi (CVE-2016-6772).
- Information disclosure vulnerability in Mediaserver (CVE-2016-6773).
- Information disclosure vulnerability in Package Manager (CVE-2016-6774) .
- Elevation of privilege vulnerability in kernel memory subsystem (CVE-2016-4794, CVE-2016-5195).
- Elevation of privilege vulnerability in NVIDIA GPU driver (CVE-2016-6775, CVE-2016-6776, CVE-2016-6777).
- Elevation of privilege vulnerability in kernel (CVE-2015-8966).
- Elevation of privilege vulnerability in NVIDIA video driver (CVE-2016-6915, CVE-2016-6916, CVE-2016-6917).
- Elevation of privilege vulnerability in kernel ION driver (CVE-2016-9120).
- Vulnerabilities in Qualcomm components (CVE-2016-8411).
- Elevation of privilege vulnerability in kernel file system (CVE-2014-4014).
- Elevation of privilege vulnerability in kernel (CVE-2015-8967).
- Elevation of privilege vulnerability in HTC sound codec driver (CVE-2016-6778, CVE-2016-6779, CVE-2016-6780).
- Elevation of privilege vulnerability in MediaTek driver (CVE-2016-6492, CVE-2016-6781, CVE-2016-6782, CVE-2016-6783, CVE-2016-6784, CVE-2016-6785).
- Elevation of privilege vulnerability in Qualcomm media codecs (CVE-2016-6761, CVE-2016-6760, CVE-2016-6759, CVE-2016-6758).
- Elevation of privilege vulnerability in Qualcomm camera driver (CVE-2016-6755).
- Elevation of privilege vulnerability in kernel performance subsystem (CVE-2016-6786, CVE-2016-6787).
- Elevation of privilege vulnerability in MediaTek I2C driver (CVE-2016-6788).
- Elevation of privilege vulnerability in NVIDIA libomx library (CVE-2016-6789, CVE-2016-6790).
- Elevation of privilege vulnerability in Qualcomm sound driver (CVE-2016-6791, CVE-2016-8391, CVE-2016-8392).
- Elevation of privilege vulnerability in kernel security subsystem (CVE-2015-7872).
- Elevation of privilege vulnerability in Synaptics touchscreen driver (CVE-2016-8393, CVE-2016-8394).
- Elevation of privilege vulnerability in Broadcom Wi-Fi driver (CVE-2014-9909, CVE-2014-9910).
- Information disclosure vulnerability in MediaTek video driver (CVE-2016-8396).
- Information disclosure vulnerability in NVIDIA video driver (CVE-2016-8397).
- Denial of service vulnerability in GPS (CVE-2016-5341).
- Denial of service vulnerability in NVIDIA camera driver (CVE-2016-8395).
- Elevation of privilege vulnerability in kernel networking subsystem (CVE-2016-8399).
- Information disclosure vulnerability in Qualcomm components (CVE-2016-6756, CVE-2016-6757).
- Information disclosure vulnerability in NVIDIA librm library (CVE-2016-8400).

- Information disclosure vulnerability in kernel components (CVE-2016-8401, CVE-2016-8402, CVE-2016-8403, CVE-2016-8404, CVE-2016-8405, CVE-2016-8406, CVE-2016-8407).
- Information disclosure vulnerability in NVIDIA video driver (CVE-2016-8408, CVE-2016-8409).
- Information disclosure vulnerability in Qualcomm sound driver (CVE-2016-8410).

Successful exploitation of these vulnerabilities could result in remote code execution in the context of the application, an attacker gaining elevated privileges, information disclosure, causing denial of service or bypassing security restrictions.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Google Android or mobile carriers to vulnerable systems, immediately after appropriate testing.
- Remind users to download apps only from trusted vendors in the Play Store.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Google:

<https://source.android.com/security/bulletin/2016-12-01.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5419>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5420>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5421>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6762>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6763>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6766>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6765>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6764>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6767>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6768>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6769>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6770>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6771>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6772>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6773>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6774>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4794>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5195>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6775>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6776>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6777>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8966>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6915>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8408>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8409>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8410>

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>